

FORM PTO-1449

Docket Number (Optional)
81942.0004Application Number
09/708,263INFORMATION DISCLOSURE CITATION
IN AN APPLICATION

Applicant

OGISHI, et al.

Filing Date

November 7, 2000

Group Art Unit

2134

(Use several sheets if necessary)

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
					YES	NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

JH	Joseph H. Silverman, "The Arithmetic of Elliptic Curves", Springer-Verlag, 1986, pp. 94-99
EX	OKAMOTO, et al., "Cipher/Zero Knowledge Proof/Number Theory", edited by Information Processing Society of Japan, Kyoritsu Suppan, 1995, pp. 185-197
QW	MENEZES, et al., "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", IEEE Trans. Inf. Theory 39, pp. 1630-1646, 1993
QZ	KANAYAMA, et al., "An Implementation of the MOV Reduction and the FR Reduction", SCIS '99, no.fl-1.4, Jan 1999, pp. 791-793
JA	BLAKE, et al., "Elliptic Curves in Cryptography", London Mathematical Society Lecture Note Series 265. Cambridge University Press, 1999, pp. 42-45, pp. 79-89
JA	HARAZAWA, et al., "Comparing the MOV and FR Reductions in Elliptic Curve Cryptography", vol.J82-A no.8, pp. 1278-1290
JA	M. KASAHARA, "Key Sharing System Based on the ID Information", vol. 47, no.2, pp. 141-145, Feb. 1993
JA	MATSUMOTO, et al., "On the Key Predistribution System: A Practical Solution to the Key Distribution Problem", Proceeding of Crypto'87, pp. 340-349, 1987
JA	H. TANAKA, "A Realization Scheme for the Identity-Based Cryptosystem", Proceeding of Crypto'87, pp. 340-349, 1987
JA	S. TSUJII, "An ID-Based Cryptosystem Based on the Discrete Logarithm Problem", IEEE Journal on Selected Areas in Communications, Vol.7, No. 4, 1989, pp. 467-473
EX	S. LANG, "Elliptic Curves Diophantine Analysis", Department of Mathematics, Yale University, Springer-Verlag. GTM112, 1978
JA	N. KOBLITZ, "Elliptic Curve Cryptosystems", Math. Comp. Vol.48. pp. 203-209. 1987
JA	V. MILLER, "Use of Elliptic Curves in Cryptography", Crypto85, pp.417-426. 1985
JA	J.A. SOLINAS, "An Improved Algorithm for Arithmetic on a Family of Elliptic Curves", Crypto97, pp. 357-371, 1997
JA	D. BAILEY, et al., "Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms", Crypto'98, pp. 472-485. 1998
JA	H. COHEN, et al., "Efficient Elliptic Curve Exponentiation Using Mixed Coordinates", AsiaCrypto'98, pp. 51-65, 1998

EXAMINER

DATE CONSIDERED

3/8/05

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.

EX
301

FORM PTO-1449

Docket Number (Optional)
81942.0004Application Number
09/708,263INFORMATION DISCLOSURE CITATION
IN AN APPLICATION

(Use several sheets if necessary)

Applicant

OGISHI, et al.

Filing Date

November 7, 2000

Group Art Unit

2134

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

On	OHGISHI, et al., "Elliptic Curve Signature Scheme With No y Coordinate", SCIS'99, pp. 51-65, 1998
On	SATOH, et al., "Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves", Comm. Math. Univ. Sancti Pauli, Vol. 47, pp. 81-92, 1998
On	N.P. SMART, "The Discrete Logarithm Problem on Elliptic Curves of Trace One", Journal of Cryptology, 1999, pp.193-196
On	I.A. SEMAEV, Evaluation of Discrete Logarithms In A Group of p -Torsion Points of An Elliptic Curve in Characteristic p , Math. Comp. Vol. 67, pp. 353-356, 1998
On	FREY, et al., "A Remark Concerning m -Divisibility and The Discrete Logarithm in the Divisor Class Group of Curves", Math. Comp. Vol. 62, pp. 865-874, 1994
On	R. SCHOOF, Elliptic Curves Over Finite Fields and the Computation of Square Roots Mod p Math. Comp. Vol. 44, pp. 482-494, 1985
On	F. MORAIN, "Building Cyclic Elliptic Curves Modulo Large Primes", EuroCrypt'91, pp. 328-336, 1991

EXAMINER

DATE CONSIDERED

3/8/05

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the applicant.